Sicherheitsanalyse RFID-basierter Wertschöpfungsketten

Eberhard Grummt[1,2] · Kerstin Werner[1] · Ralf Ackermann[1]

[1]SAP Research CEC Dresden
{eberhard.oliver.grummt | kerstin.werner | ralf.ackermann}@sap.com

[2]Technische Universität Dresden, Professur Rechnernetze

Zusammenfassung

In globalen Wertschöpfungsketten agierende Unternehmen erkennen zunehmend das Potenzial der RFID-Technologie als Basis für Prozessoptimierungen im Supply Chain Management. Ein flächendeckender Einsatz ist jedoch noch nicht zu verzeichnen, was neben Aspekten der Standardisierung und der Kosten nicht zuletzt durch Sicherheitsprobleme begründet ist. Dieser Beitrag beleuchtet potenzielle Schwachstellen und mögliche Lösungen in RFID-basierten, kooperativen Wertschöpfungsketten auf Basis eines neuen, generischen Architektur-Modells. Dieses umfasst neben einer technischen Sicht auf die zur Erfassung, Verwaltung und kooperativen Nutzung der Informationen notwendigen IT-Systeme auch eine organisatorische Sicht. Diese bezieht unter anderem den physischen Austausch von Transpondern und Abhängigkeiten zu externen Dienstleistern mit ein.

1 Einführung

Die RFID (Radio Frequency Identification)-Technologie ermöglicht das automatische Erkennen von Objekten durch maschinelles Auslesen an ihnen befestigter Funk-Transponder (*Tags*). Gegenüber dem traditionellen Barcode bietet RFID Vorteile hinsichtlich Geschwindigkeit, Speicherkapazität, Fälschungssicherheit, Wiederverwendbarkeit, Wiederbeschreibbarkeit und des entfernten Auslesens ohne Sichtverbindung. Besonders im Bereich des Supply Chain Managements haben diese Eigenschaften und ein stetiger Preisverfall dazu geführt, dass diese Technologie zunehmende Verbreitung findet. Während der innerbetriebliche Einsatz (*closed loop*) schon seit über zehn Jahren Realität ist [TD06], ist die flächendeckende überbetriebliche Verwendung von RFID entlang der gesamten Wertschöpfungskette (*open loop*) noch eine Zukunftsvision.

Obwohl unternehmensübergreifender Austausch von Informationen, die Güter in gemeinsam verwalteten Wertschöpfungsketten betreffen, ein hohes Potenzial für Effizienzsteigerungen und Kostensenkungen verspricht, birgt er auch Risiken und Probleme. Zum einen ist es organisatorisch als auch technisch problematisch, den optimalen Grad der Informationstransparenz zwischen Kooperationspartnern zu bestimmen und durchzusetzen [Str05]. Zum anderen sind einzelne Systemteile und Übertragungskanäle externen Angreifern ausgesetzt.

In dieser Arbeit wird ein allgemeines Architektur-Modell für die Beschreibung von RFID-

Diese Arbeit wurde teilweise unterstützt durch das Bundesministerium für Wirtschaft und Technologie im Rahmen des Projekts Ko-RFID

gestützten Wertschöpfungsketten sowohl auf organisatorischer als auch auf technischer Ebene (Abschnitt 2) entwickelt. In diesem werden sowohl die Güter- und Datenflüsse zwischen den beteiligten Unternehmen (horizontale Sicht), die innerbetrieblichen Datenflüsse (vertikale Sicht) als auch die Abhängigkeiten zu dritten Parteien berücksichtigt. Anschließend werden potenzielle Schwachstellen und Sicherheitsrisiken innerbetrieblicher (Abschnitt 3), unternehmensübergreifender (Abschnitt 4) und externer Systeme (Abschnitt 5) anhand des erstellten Modells beschrieben sowie daraus folgende Implikationen diskutiert.

2 Modell RFID-basierter Wertschöpfungsketten

In diesem Kapitel wird auf Basis von Fallstudien zunächst ein abstraktes Modell für Wertschöpfungsketten entwickelt. Anschließend wird ein Modell für Informationssysteme vorgestellt, welche von Teilnehmern RFID-gestützter Wertschöpfungsketten umgesetzt werden, um die Interoperabilität zu gewährleisten. Danach werden zum Betrieb des Systems benötigte externe Dienste wie Verzeichnis- und Authentifizierungsdienste eingeführt, um abschließend ein ganzheitliches Modell vorzustellen. Als Voraussetzung wird die Annahme getroffen, dass jedes RFID-Tag mit einem eineindeutigen, von allen Partnern decodierbaren Identifizierungscode (*ID*) ausgestattet ist, d.h. ein globales Nummerierungsschema existiert.

2.1 Modellierung der Wertschöpfungskette

Um Wertschöpfungsketten in einem abstrakten Modell generisch darzustellen, wurden verschiedene Beispiele und Fallstudien [MRvR$^+$05, Ste06b, Ste06a] untersucht, woraus sich ergab, dass in jedem Fall minimal zwei Unternehmen an einer Wertschöpfungskette beteiligt sein müssen. Eines schickt eine bestimmte Lieferung in Umlauf (Ursprungsunternehmen oder Quelle) und ein anderes empfängt sie (Zielunternehmen oder Senke). Reale Wertschöpfungsketten bestehen jedoch zumeist aus mehreren Partnern, denn zwischen Ursprungs- und Zielunternehmen können Lieferungen weitere variable Partner passieren, wie beispielsweise Transportunternehmen, Weiterverarbeitungsbetriebe oder Verteilzentren. Der beschriebene Sachverhalt wird in Abbildung 1 dargestellt, indem Unternehmen 1 und Unternehmen n, die beiden stets vorhandenen Bestandteile von Wertschöpfungsketten, links bzw. rechts abgebildet sind. Zwischen ihnen befindet sich ein Platzhalter für $n - 2$ potenzielle weitere Partner.

Es wurde bereits viel Arbeit dahingehend geleistet, entstehende Bedrohungen bezüglich Datenschutz und Datensicherheit für Endverbraucher zu analysieren und einzuschränken [GJP05, Lan05, GS05]. Ziel des vorliegenden Beitrags ist es hingegen, ausschließlich die Belange von Unternehmen stärker zu beleuchten.

2.2 Modellierung RFID-gestützter Informationssysteme

Ein RFID-gestütztes Informationssystem muss diverse Kernfunktionalitäten bereitstellen. So müssen Tags von Lesegeräten gelesen und ggf. beschrieben, Leseereignisse gefiltert, aggregiert und semantisch angereichert („vorverarbeitet“) sowie diese erweiterten Ereignisse gespeichert werden. Um ihren Austausch mit internen und externen Anwendungen zu ermöglichen, werden Abfrageschnittstellen benötigt. Darüber hinaus ist eine *Anwendungs-Ebene* vorzusehen, die Applikationen zur Steuerung der Funktionalitäten unterer Ebenen sowie zur Steuerung und Überwachung von Geschäftsprozessen beinhaltet. Tabelle 1 fasst die Ebenen und die dort bereitgestellten Funktionalitäten zusammen.

Um einen unternehmensübergreifenden Datenaustausch zwischen beliebigen Unternehmen zu

Tab. 1: Funktionalitäten und Ebenen des Modells

Ebene	Funktionalität
(1) Tag-Ebene	Physisches Bereitstellen von Tags
(2) Sensor-Ebene	Lesen und ggf. Schreiben von RFID-Tags
(3) Aufbereitungs-Ebene	Puffern, Formatieren, Filtern, Aggregieren von Leseereignissen
(4) Persistenz-Ebene	Speichern relevanter Daten
(5) Austausch-Ebene	Bereitstellung von Abfrageschnittstellen für interne und externe Systeme
(6) Anwendungs-Ebene	Bereitstellung von Anwendungen

ermöglichen, werden neben der Einhaltung bestimmter Daten- und Schnittstellenkonventionen zwei externe Kerndienste benötigt: ein *Authentifizierungsdienst* und ein *Auffindungsdienst*. Diese müssen von „vertrauenswürdigen Dritten“ betrieben werden. Das Modell sieht vor, dass Unternehmen Informationen sowohl auf Basis eigener als auch auf Basis fremder Leseereignisse in ihrer *Persistenz-Ebene* integrieren. Bei welchen Unternehmen Informationen zu einem spezifischen Tag gespeichert sind, kann über einen externen Auffindungsdienst in Erfahrung gebracht werden (diese Architektur entspricht dem *Metadata Integration Server approach* aus [DAH06]). Es existieren darüber hinaus weitere Ansätze, z.B. kann die Persistenz-Ebene als zentrale, von mehreren Unternehmen genutzte Datenbank modelliert werden.

2.3 Ganzheitliche Modellierung

Die vorgestellten Modelle für Wertschöpfungsketten und Informationssysteme wurden in ein ganzheitliches Modell integriert (siehe Abbildung 1). Zahlen kennzeichnen Teile der unternehmensinternen IT-Systeme, Buchstaben kennzeichnen Datenflüsse in oder zwischen Unternehmen. Im Falle von (F) werden auch physische Objekte, d.h. Güter mit ihren RFID-Tags ausgetauscht. Auf die externen Dienste greifen üblicherweise alle Teilnehmer der Wertschöpfungskette zu (über I und H), aus Übersichtlichkeitsgründen sind die entsprechenden Pfeile aber nur bei Unternehmen 1 eingezeichnet. Gleiches gilt für die Austauschebenen (5), über die alle Teilnehmer netzartig kommunizieren (G).

Ein Datenfluss findet hauptsächlich auf der *Tag-Ebene* (1) und auf der *Austausch-Ebene* (5) statt. Ein Austausch auf anderen Ebenen wie z.B. der *Sensor*-(2) oder *Aufbereitungs-Ebene* (3) [RF06] ist prinzipiell denkbar, aber unüblich.

3 Sicherheitsanalyse innerbetrieblicher Systeme

Anhand der modellierten innerbetrieblichen Systemteile werden nun spezifische Bedrohungen und Ansätze zu deren Minimierung beschrieben.

3.1 Tag-Ebene

Ohne entsprechenden Schutz können Transponder (1) innerhalb einer bestimmten Reichweite von kompatiblen Lesegeräten ausgelesen werden. Wenn Angreifer an verschiedenen Stellen von Wertschöpfungsketten die eindeutige Identifikationsnummer eines Transponders auslesen, können sie Lieferbeziehungen aufdecken und ermitteln, wann sich ein Objekt bei wem und wie lange aufhält. Ebenso besteht die Möglichkeit, dass Angreifer sich Tags bemächtigen, die entsorgt oder an Verbraucher übergeben, aber nicht zerstört wurden. Dies ist eine weitere Möglichkeit dar, an gespeicherte, vertrauliche Informationen zu gelangen. Eine andere Gefah-

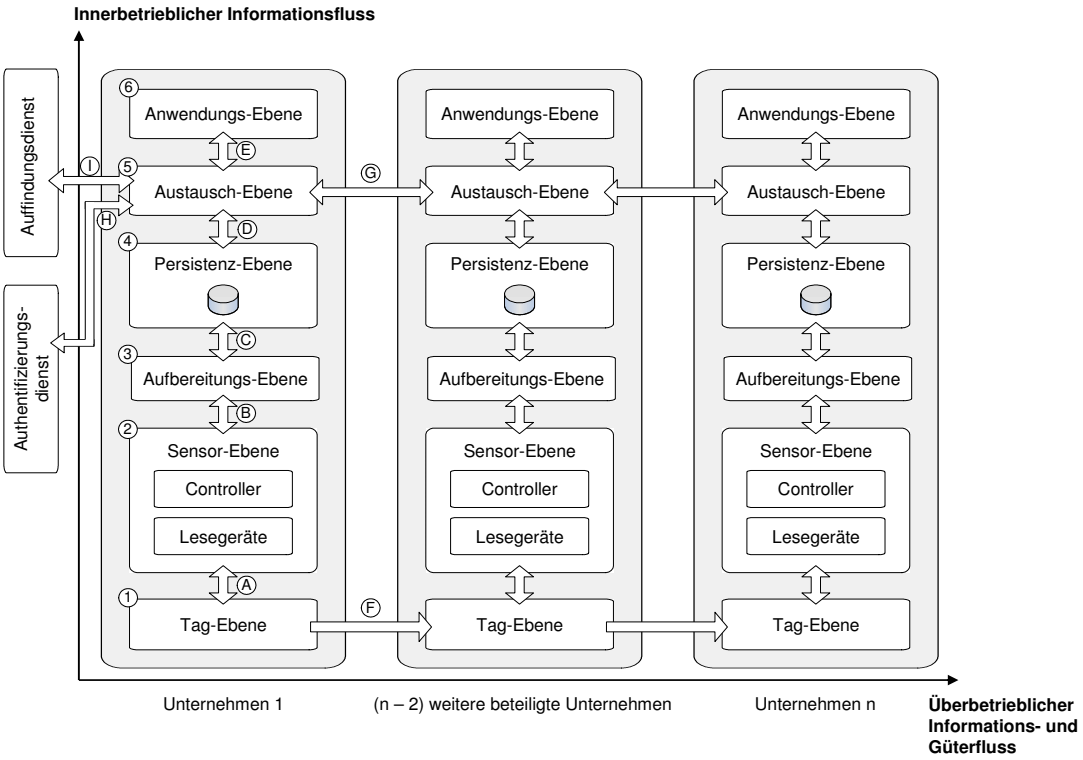

Abb. 1: Modell einer generischen RFID-gestützten Wertschöpfungskette

renquelle stellen Hersteller von Tags dar, da sie ihre Produkte beispielsweise mit unerwähnten Speicherbereichen oder manipulierter Killfunktionalität [Aut02] ausstatten könnten, um zu gegebenem Zeitpunkt zerstört geglaubte Informationen auszulesen.
Gelingt es einem Angreifer, ein oder mehrere Tags einer Lieferung mit falschen Informationen, z.B. einer falschen Herstellerkennung, zu beschreiben, kann er ohne entsprechenden Schutz unerkannt falsche Informationen in das System einschleusen. Ein anderer Weg, dies zu erreichen, ist das Einschleusen präparierter Transponder in den Güterfluss. Auf diese Weise kann z.B. die Lieferung unbestellter Produkte vorgetäuscht werden. Eine weitere Möglichkeit ist es, entsorgte oder an Verbraucher übergebene, aber nicht deaktivierte Transponder wieder in die Wertschöpfungskette einzubringen.
Sofern die physische Verbindung zwischen Trägerobjekt und Transponder nicht sicher gewährleistet ist, kann ein Angreifer Transponder von einem Objekt an einem anderen anbringen und so die Anwesenheit eines längst entwendeten Objektes suggerieren oder das Vorhandensein eines Objektes an unerwarteten Orten vortäuschen. Auf diese Weise fallen in oberen Systemebenen mit der Realität inkonsistente Daten an.
In [RCT06] und [rfi] wird beschrieben, wie über präparierte Transponder ein „RFID-Virus“ in ein System eingeschleust werden kann. Dieser bewirkte einen Absturz der angeschlossenen Datenhaltung und pflanzte sich auf alle im Anschluss gelesenen Tags des infizierten Systems fort. Durch einen solchen Angriff kann prinzipiell eine Schadfunktion in einer gesamten Wertschöpfungskette verbreitet werden. Um ihn durchzuführen müssen entweder wiederbeschreibbare Tags innerhalb der Wertschöpfungskette für einen Angreifer zugänglich sein, oder es gelingt ihm, bereits präparierte Tags in den Güterfluss einzubringen.
So genannte *Blocker Tags* [JRS03] können versteckt angebracht dazu verwendet werden, andere

in ihrer Nähe befindliche Tags vor der Erkennung durch ein Lesegerät abzuschirmen. Eine weitere Möglichkeit, Transponder vor einem Lesegerät abzuschirmen, bietet die Verwendung von Metallfolie oder metallisierten Aufklebern, die über abzuschirmenden Tags angebracht werden. Tags können darüber hinaus chemisch, physisch oder durch elektromagnetische Einwirkung, wie beispielsweise durch den in [zap] vorgestellten *RFID-Zapper*, zerstört werden.
Aktive Transponder bieten innerhalb der Wertschöpfungskette einen spezifischen Angriffspunkt, da sie durch übermäßige Lese- und Schreibanfragen vorzeitig entladen und unbrauchbar gemacht werden können. Die Kommunikation zwischen Tags und Lesegeräten der Sensorebene über die Luftschnittstelle (A) kann von Angreifern innerhalb einer bestimmten Reichweite, sofern keine entsprechenden Schutzmaßnahmen ergriffen wurden, mitgehört werden. Es gilt allerdings zu unterscheiden, in welcher Richtung sensible Informationen gesendet werden. Werden sie auf dem Hinkanal, also vom Lesegerät an das Tag gesendet, können sie aufgrund der größeren Signalstärke über weitere Distanzen abgehört werden als auf dem Rückkanal. Geht es lediglich darum aufzudecken, ob überhaupt eine Kommunikation zwischen den beiden Komponenten stattfindet, können Angreifer versuchen zu ermitteln, ob ein elektromagnetisches Feld zwischen ihnen besteht. Wie bei allen ungeschützten Übertragungswegen können auch hier Man-in-the-Middle-Angriffe bzw. Maskeraden durchgeführt werden. Übertragene Informationen können von Angreifern modifiziert oder gelöscht werden. Die Verfügbarkeit der Luftschnittstelle kann beispielsweise durch die Verwendung eines Störsenders in der Umgebung eingeschränkt werden. Des Weiteren können übermäßig viele Daten eingespeist und somit Denial-of-Service-Angriffe durchgeführt werden.

Die angeführten Bedrohungen sollten durch die Wahl geeigneter Schutzmaßnahmen berücksichtig werden. Diesbezüglich können beispielsweise Zugriffsschutzverfahren [JRS03], Verschlüsselung gespeicherter Informationen [Jue04], Anonymisierung oder Pseudonymisierung [Lan05] als auch physischer Schutz [Bun05] zum Einsatz kommen.

3.2 Sensor-Ebene

Für Komponenten der Sensor-Ebene (2) gilt es zu unterscheiden, welche Abmessungen sie haben. Kleinere Geräte können von Angreifern leichter als größere entfernt und z.B. gegen präparierte Einheiten ausgetauscht werden. Auf diese Weise kann nicht dokumentierte Funktionalität eingeschleust werden. Allerdings können Hersteller dieser Komponenten einen solchen Angriff ebenfalls bei größeren stationären Geräten durchführen.
Ein präpariertes oder vom Angreifer ausgetauschtes Lesegerät kann falsche Informationen auf Tags schreiben bzw. falsche oder unvollständige Informationen über den Device-Controller an höher gelegene Ebenen senden. Ein unberechtigtes Gerät kann darüber hinaus die Identität eines Berechtigten vortäuschen und anschließend falsche oder unvollständige Daten auf Transponder schreiben bzw. an höhere Ebenen schicken. Verfälschte Informationen können ebenso bereits in oberen Ebenen entstanden sein. Deshalb sollten Controller und Lesegeräte die von der Aufbereitungsebene empfangenen Daten überprüfen, bevor sie diese verarbeiten.
Von einem Angreifer präparierte Lesegeräte oder Controller können dazu verwendet werden, übermäßig viele Lese- und Schreibanfragen an Transponder zu senden, wodurch batteriebetriebene Tags entladen und unbrauchbar gemacht werden können. Die Verfügbarkeit der Geräte kann durch Angreifer zusätzlich gefährdet werden, indem der entsprechende Port oder die Kontaktverbindungen zur Energieversorgung sowie zur höher gelegenen Ebene physisch oder chemisch zerstört werden.
Die Kommunikation zwischen Sensor- und Aufbereitungsebene (B) kann von Angreifern mit-

gehört werden. Wie bereits unter 3.1 beschrieben wurde, können auch hier Man-in-the-Middle-Angriffe bzw. Maskeraden durchgeführt und übertragene Informationen verändert oder gelöscht werden. Des Weiteren können Übertragungswege beschädigt oder sogar durchtrennt werden, sofern ein ungeschützter Zugriff auf sie besteht.

3.3 Aufbereitungs-Ebene

Die Aufbereitungs-Ebene kann als Middleware betrachtet werden, die auf einem oder mehreren Applikationsservern betrieben wird. Diese sind somit den bekannten Risiken durch unerlaubten Zugriff, Schadsoftware und Denial-of-Service-Attacken ausgesetzt. Direkten Zugriff kann sich ein Angreifer durch Passwort-Attacken, Code-Injection, Buffer-Overflows, Viren, Würmer und Trojaner sowie durch physischen Zugriff und Social Engineering verschaffen. Weiterhin kann er versuchen, Informationen an den Schnittstellen zur Sensor-Ebene und zur Persistenz-Ebene zu erlangen. Spezifische Angriffe können durch bewusstes Einschleusen von präparierten Eingabedaten über die Sensor-Ebene (bzw. transitiv über die Tag-Ebene [RCT06]) durchgeführt werden. Als Ansätze sind Buffer-Overflows [CWP+00] und SQL-Injections [HVO06] zu nennen. Auch können speziell präparierte Sensorinformationen in Verbindung mit internen Verarbeitungsregeln in unvorhergesehener Weise interagieren und so z.B. Endlos-Verarbeitungsschleifen als auch widersprüchliche oder unerwartete Entscheidungen auslösen. Extrem große Mengen an Eingabedaten, z.B. von präparierten RFID-Readern oder Transpondern, können außerdem die Verfügbarkeit beeinträchtigen, indem sie das System verlangsamen oder zum Absturz bringen.
Gegenmaßnahmen umfassen neben physischer Sicherung Zugriffskontrollen mit starken Schlüsseln/Passwörtern und Authentifizierung über Zertifikate, regelmäßige Backups, redundante Datenhaltung, Firewalls, Log-Dateien und Intrusion Detection-Systeme. Empfehlenswert ist darüber hinaus die gegenseitige Authentifizierung angebundener Systeme der Sensor- und Persistenz-Ebene sowie eine verschlüsselte Datenübertragung, wenn ein Abhören nicht durch physische Maßnahmen unterbunden werden kann, z.B. wenn ein öffentliches Netz als Übertragungsmedium genutzt wird.

3.4 Persistenz-Ebene

Für die persistente Datenhaltung werden vorrangig relationale Datenbanken eingesetzt. Die entsprechenden Datenbank-Server sind ähnlichen Angriffen wie der Applikationsserver der Aufbereitungsebene ausgesetzt. Wird keine angemessene Überprüfung und Filterung der Ereignisdaten der Aufbereitungsebene durchgeführt, kann die (referenzielle) Integrität der Daten angegriffen werden oder gar Schadcode (SQL-Injections) eingeführt werden.
Redundanz und räumliche Verteilung der Datenbankserver kann helfen, die Sicherheit gegen physische Angriffe zu erhöhen.

3.5 Austausch-Ebene

Die Austausch-Ebene stellt Schnittstellen zu unternehmensinternen und -externen Systemen bereit. Auch hier treffen die im Kontext der Aufbereitungs- und Persistenz-Ebene genannten Bedrohungen der Serversicherheit sowie deren Minimierungsansätze zu. Weitere Bedrohungen werden in Abschnitt 4.2 behandelt.

4 Unternehmensübergreifende Systeme

In den folgenden Abschnitten wird die horizontale Informationsübermittlung auf Tag-Ebene (F) sowie auf Austausch-Ebene (G) hinsichtlich Bedrohungen der Datensicherheit analysiert.

4.1 Tag-Ebene

Da auf Transpondern Informationen gespeichert werden und sie mit Trägerobjekten innerhalb von Lieferungen zwischen Partnerunternehmen ausgetauscht werden, findet gleichzeitig eine Informationsübertragung (F) statt. Die übermittelten Informationen unterliegen einerseits den unter 3.1 genannten Bedrohungen und andererseits den Einflüssen, welche sich durch den Kontakt mit diversen Besitzern ergeben. Als Angreifer kommen dadurch nicht nur unternehmensinterne Mitarbeiter oder Eindringlinge in Frage, sondern alle Personen und Systeme, welche entlang der vorhandenen Lieferbeziehungen in ausreichende Nähe von Transpondern gelangen können. Eine Besonderheit besteht allerdings darin, dass Informationen ausschließlich an dem Ort zur Verfügung stehen, an welchem sich Transponder jeweils befinden.
Es gilt zu unterscheiden, ob auf Tags lediglich eine ID (*Data-on-Network*) oder darüber hinaus zusätzliche Informationen (*Data-on-Tag*) gespeichert werden. Die Ermittlung oder gar Verfolgung von Transpondern anhand ihrer ID erlaubt es Angreifern, Mengen, Lieferbeziehungen und Aufenthaltszeiträume in Erfahrung zu bringen. Werden weitere Daten auf Tags gespeichert, entsteht dadurch bezüglich deren Vertraulichkeit, Integrität und Verfügbarkeit eine zusätzliche Bedrohung, welche durch Maßnahmen, wie sie bereits unter 3.1 beschrieben wurden berücksichtigt werden sollten. Zusätzlich müssen hier jedoch die multilateralen Anforderungen der verschiedenen teilnehmenden Unternehmen beachtet werden, was beispielsweise auf einzusetzende Zugriffskontrollen Auswirkungen hat.

4.2 Austausch-Ebene

Bezüglich der externen Schnittstelle der Austausch-Ebene (G) ist insbesondere die Gefahr des unerlaubten lesenden oder schreibenden Zugriffs von externen Angreifern zu adressieren. Denn nur hier und auf der Tag-Ebene werden externen Teilnehmern explizit Zugriffsmöglichkeiten bereitgestellt, die damit auch für Unbefugte einen attraktiven Angriffspunkt, z.B. für Passwort- und Spoofing-Attacken darstellen. Der Zugriff kann direkt auf das System erfolgen oder auf den Netzwerkverkehr, wenn dieser über öffentliche Netze wie das Internet stattfindet. Haben sich externe Angreifer Zugriff zum System verschafft, können sie vertrauliche Informationen auslesen, gefälschte Daten oder gar Programmcode einschleusen.
Zugriffskontrollsysteme mit starker Authentifizierung, Signaturen, starke Passwörter und Verschlüsselung, Firewalls und Demilitarisierte Zonen (DMZ) sowie sorgfältige Prüfung der Eingabedaten sind wichtige Aspekte der Sicherung von Systemen der Austausch-Ebene. Generell treffen bereits diskutierte Aspekte der Serversicherheit auch auf die Austausch-Ebene zu. Grundlegende Entwurfsprinzipien wie Datensparsamkeit und geringstmögliche Privilegierung sollten bereits beim Systemdesign berücksichtigt werden. Bei der potenziell sehr großen Menge an Informationen, verschiedenen feingranularen Berechtigungen und Teilnehmern ist dies mit momentan verfügbaren Verfahren wie rollenbasierter Zugriffskontrolle und manueller Verwaltung von Zertifikaten und Login-Daten nur schwer zu erreichen.

5 Systeme externer Dienstleister

Die benötigten Auffindungs- und Authentifizierungsdienste werden von externen Dienstleistern angeboten. Der Auffindungsdienst ist im Wesentlichen ein Verzeichnisdienst, der Metadaten (Adressen) zu Informationen, die bestimmte RFID-Tags betreffen, speichert. Auf eine Anfrage der Form „Wo finde ich Informationen zu Tag Nr. 84590235?“ antwortet der Dienst mit einer Liste von Verweisen auf Dienste der Austausch-Ebene von Firmen, die Informationen zu

diesem Tag besitzen. Dadurch kann der Betreiber des Auffindungsdienstes umfangreiche Lieferbeziehungen aufdecken und somit die Vertraulichkeit dieser Informationen kompromittieren. Werden Anfragen generell beantwortet, kann dies ebenso ein beliebiges externes System tun. Soll vor Beantwortung einer Anfrage geprüft werden, ob der Anfragende dazu berechtigt ist, müssen unter Umständen zahlreiche Zugriffs-Policies unterschiedlicher Unternehmen ausgewertet werden.

Ist die Verfügbarkeit des Auffindungsdienstes oder des Authentifizierungsdienstes beeinträchtigt, können davon abhängige Unternehmen starke Funktionalitätseinbußen und damit finanziellen Schaden erleiden.

Die Sicherstellung der Authentizität der Betreiber selbst sowie der Integrität gelieferter Daten ist von großer Bedeutung. Kann ein Angreifer den Auffindungsdienst kompromittieren, kann er Unternehmen auf gefälschte Informationen weiterleiten (analog zu Angriffen mit gefälschten DNS-Einträgen), welche die Geschäftsprozesse des Betroffenen signifikant beeinträchtigen können (insbesondere bei hohem Automatisierungsgrad z.B. der Produktion).

6 Verwandte Arbeiten

Konidala et al. [KKK07] geben einen Überblick über die EPC-Netzwerk-Architektur und diskutieren potenzielle Sicherheitsprobleme und deren Lösungen an den einzelnen Stationen der Informationsverarbeitungskette. Die Schwächen des vom Industriekonsortium EPCglobal[1] vorgeschlagenen, auf dem *Domain Name System* (DNS) basierenden Auffindungsdienst *Object Name Service* (ONS) werden in [FGS05] diskutiert. In der Studie „Risiken und Chancen des Einsatzes von RFID-Systemen“ [Bun05] des Bundesamt für Sicherheit in der Informationstechnik (BSI) werden Bedrohungen und Lösungsansätze insbesondere auf Tag-, Luftschnittstellen- und Reader-Ebene beleuchtet. Weitere technische Betrachtungen von Aspekten der Datensicherheit und des Datenschutzes finden sich z.B. in [Jue06, PHER06].

7 Zusammenfassung und Ausblick

Die in diesem Beitrag durchgeführte Sicherheitsanalyse hat gezeigt, dass RFID-Transponder ein schwaches Glied innerhalb der betrachteten Systembestandteile darstellen. Durch sie sollen Informationen in Verbindung mit Gütern durch Wertschöpfungsketten transportiert und Zustandsinformationen in nahezu Echtzeit ermittelt werden. Dies hat zur Folge, dass sie nicht wie andere Bestandteile ausschließlich in einer vertraulichen, gut geschützten und überwachten Umgebung aufbewahrt werden können, sondern sich zusätzlich physisch zwischen Unternehmenspartnern bewegen. Dies in Verbindung mit der Möglichkeit des kontaktlosen, entfernten Auslesens vereinfacht bestimmte Angriffe erheblich. Deshalb spielt die Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit auf Tag-Ebene durch entsprechende Schutzmaßnahmen, wie sie unter 3.1 und 4.1 genannt wurden, eine sehr wichtige Rolle. Andererseits kann die Notwendigkeit für den Angreifer, sich Tags physisch anzunähern, als Sicherheitsmerkmal gesehen werden. Anders als auf Netzwerke kann der Angriff also nicht von jeder beliebigen physischen Lokation mit Netzwerkzugang durchgeführt werden. Bei der Wahl geeigneter Maßnahmen gilt es gleichzeitig die in diesem Beitrag nicht betrachteten Verbraucherängste hinsichtlich des Datenschutzes zu berücksichtigen. Auf diese Weise könnte die Akzeptanz der Technologie positiv beeinflusst werden.

[1] http://www.epcglobalinc.org

Das beschriebene ganzheitliche Architekturmodell stellt eine generische Beschreibung RFID-basierter Wertschöpfungsketten dar. Es ermöglicht, konkrete Ausprägungen einzuordnen und bestehende Risiken zu erkennen. Die Zusammenarbeit zwischen Unternehmen in Wertschöpfungsnetzen spielt zunehmend eine wichtige Rolle. Dadurch entstehende Potenziale können besser ausgeschöpft werden, wenn vorhandene Sicherheitsrisiken gezielt durch geeignete Maßnahmen berücksichtigt werden.

In höheren Ebenen findet eine semantische Anreicherung der von RFID-Reader erzeugten Leseereignisse statt. Sie werden z.B. mit Geschäftsprozessen assoziiert. Auf diesen Abstraktionebenen spielt es keine Rolle mehr, mit Hilfe welcher Auto-ID-Technolgie die Daten ursprünglich erfasst wurden. Potenzielle Sicherheitsrisiken und entsprechende Gegenmaßnahmen sind also nicht mehr RFID-spezifisch, sondern im Bereich der klassischen Server- und Netzwerksicherheit zu suchen. Jedoch ist zu berücksichtigen, dass reale Angriffe und tatsächliches Versagen von Gesamtsystemen meist Ergebnis unerwarteter Interaktionen zwischen Systemteilen sind. Deshalb sollten diese in zukünftigen Arbeiten stärker beleuchtet werden.

Zahlreiche sicherheitsrelevante Fragestellungen, die auf den vorgestellten Systemebenen angesiedelt werden können, sind dennoch ungeklärt.

Die im Logistik-Umfeld aufgrund der automatischen Erfassung anfallenden großen Datenmengen führen zu Problemen der manuellen Vergabe von Zugriffsrechten und gleichzeitiger Berücksichtigung von Entwurfsprinzipien wie „gerinstmögliche Privilegierung“ und „Datensparsamkeit“. Bestimmte Teilnehmer sollen z.B. nur Teile der verfügbaren Informationen über bestimmte Produkte erhalten. Daraus leiten sich interessante Forschungsfragen ab, z.B. wie die Zugriffsrechts-Anforderungen verschiedener Teilnehmer mehrseitig sicher berücksichtigt und Kompromisse ausgehandelt werden können. Auch werfen die großen Datenmengen und die Forderung nach feingranularer Zugriffskontrolle Fragen bzgl. der Modellierung und der Handhabbarkeit von Zugriffsrechten auf.

Die kooperative, firmenübergreifende Nutzung von RFID-Infrastrukturen stellt Herausforderungen an Interoperabilität von Systemen, aber auch an das Vertrauen zwischen einzelnen Teilnehmern. Daraus ergibt sich die interessante Frage, wie Vertrauensverhältnisse in solch einem dynamischen Kontext erfolgreich etabliert, formalisiert und für die Ableitung geltender Regeln für konkrete Kooperation genutzt werden können.

Bezüglich der externen Anbieter von Authentifizierungs- und Auffindungsdiensten sind interessante Fragestellungen, wie die Abhängigkeit von einzelnen Dienstleistern verringert und wie verhindert werden kann, dass dortige Insider Informationen aufdecken und weitergeben können. Als Ziel sollte dabei eine zuverlässige, ausfallsichere Infrastruktur gelten, in der einzelnen Anbietern nur minimal vertraut werden muss.

Literatur

[Aut02] Auto-ID Center. 860 mhz – 930 mhz class 1 radio frequency (rf) identification tag radio frequency & logical communication interface specification. Technical report, Auto-ID Center/EPCglobal, 2002.

[Bun05] Bundesamt für Sicherheit in der Informationstechnik. Risiken und chancen des einsatzes von RFID-systemen (rikcha) - trends und entwicklungen in technologien, anwendungen und sicherheit. http://www.bsi.bund.de/fachthem/rfid/RIKCHA.pdf, 2005.

[CWP+00] C. Cowan, F. Wagle, C. Pu, S. Beattie, and J. Walpole. Buffer overflows: attacks and defenses for the vulnerability of thedecade. In *DARPA Information Survivability Conference and Exposition, 2000 (DISCEX '00)*, volume 2, pages 119–129, 2000.

[DAH06] Hong-Hai Do, Jürgen Anke, and Gregor Hackenbroich. Architecture evaluation for distributed auto-id systems. In *DEXA '06: Proceedings of the 17th International Conference on Database and Expert Systems Applications*, pages 30–34, Washington, DC, USA, 2006. IEEE Computer Society.

[FGS05] Benjamin Fabian, Oliver Günther, and Sarah Spiekermann. Security analysis of the object name service for RFID. In *International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing – SecPerU'05*, Santorini Island, Greece, July 2005. IEEE, IEEE Computer Society Press.

[GJP05] Simson Garfinkel, Ari Juels, and Ravi Pappu. RFID privacy: An overview of problems and proposed solutions. *IEEE Security and Privacy*, 3(3):34–43, May-June 2005.

[GS05] Oliver Günther and Sarah Spiekermann. Rfid and the perception of control: the consumer's view. *Commun. ACM*, 48(9):73–76, 2005.

[HVO06] W. G. Halfond, J. Viegas, and A. Orso. A classification of sql-injection attacks and countermeasures. In *Proc. of the Intern. Symposium on Secure Software Engineering (ISSSE 2006)*, 2006.

[JRS03] Ari Juels, Ronald Rivest, and Michael Szydlo. The blocker tag: Selective blocking of RFID tags for consumer privacy. In Vijay Atluri, editor, *Conference on Computer and Communications Security – ACM CCS*, pages 103–111, Washington, DC, USA, October 2003. ACM, ACM Press.

[Jue04] Ari Juels. Minimalist cryptography for rfid tags. In *Security in Communication Networks*, pages 149–164. Springer Verlag, 2004.

[Jue06] Ari Juels. RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications*, 24(2):381–394, February 2006.

[KKK07] Divyan M. Konidala, Woan-Sik Kim, and Kwangjo Kim. Security assessment of epcglobal architecture framework. Technical report, Auto-ID Labs, 2007.

[Lan05] Marc Langheinrich. Die privatsphäre im ubiquitous computing – datenschutzaspekte der rfid-technologie. In Elgar Fleisch and Friedemann Mattern, editors, *Das Internet der Dinge – Ubiquitous Computing und RFID in der Praxis*, pages 329–362. Springer-Verlag, 2005.

[MRvR+05] Martin Mähler, Kurt N. Rindle, Armgard von Reden, Christian Muszynski, Christoph Weiss, and Gerd Wolfram. Rfid - motor für innovationen, Oktober 2005.

[PHER06] Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan Estevez-Tapiador, and Arturo Ribagorda. RFID systems: A survey on security threats and proposed solutions. In *11th IFIP International Conference on Personal Wireless Communications – PWC'06*, volume 4217 of *Lecture Notes in Computer Science*, pages 159–170. Springer-Verlag, September 2006.

[RCT06] Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum. Is your cat infected with a computer virus? In *Proc. 4th IEEE Intl. Conf. on Pervasive Computing and Communications*, 2006.

[RF06] Christof Roduner and Christian Floerkemeier. Towards an enterprise location service. In *SAINT-W '06: Proceedings of the International Symposium on Applications on Internet Workshops*, pages 84–87, Washington, DC, USA, 2006. IEEE Computer Society.

[rfi] http://www.rfidvirus.org/index.html. Zugriff: 08.01.2007.

[Ste06a] Steinbeis Transferzentrum My eBusiness. Fallstudie: Kaufhof warenhaus ag, gerry weber, August 2006.

[Ste06b] Steinbeis Transferzentrum My eBusiness. Fallstudie: Metro rfid-roll-out, April 2006.

[Str05] Martin Strassner. *RFID im Supply Chain Management - Auswirkungen und Handlungsempfehlungen am Beispiel der Automobilindustrie*. PhD thesis, Universität St.Gallen, Hochschule für Wirtschafts-, Rechts- und Sozialwissenschaften (HSG), 2005.

[TD06] Frédéric Thiesse and Markus Dierkes. Lottrack: Echtzeitlokalisierung in der halbleiterfertigung. *PPS Management*, 1 'RFID in Produktion und Logistik':20–23, 2006.

[zap] https://events.ccc.de/congress/2005/wiki/rfid-zapper. Zugriff: 12.11.2006.